Seminar Nasional Sains dan Teknologi Informasi (SENSASI)
SENSASI 2021
ISBN: 978-623-93614-6-4
Agustus 2021
Hal: 103 - 107

Perancangan Protection Profile untuk Standalone File Encryption berdasarkan SNI ISO/IEC 15408:2014

Esti Rahmawati Agustina*, Yhufi Swastantri Gustiviana

Badan Siber dan Sandi Negara, Depok, Jawa Barat, Indonesia
Email: 1,*esti.rahmawati@bssn.go.id, 2yhufi.swastantri@bssn.go.id

Abstrak

Fasilitasi standardisasi keamanan perangkat teknologi informasi (TI) merupakan salah satu layanan yang diberikan oleh Badan Siber dan Sandi Negara. Salah satu bentuk pelaksanaan standardisasi keamanan perangkat TI berupa penyusunan *Protection Profile* (PP). PP merupakan dokumen yang berisi sekumpulan persyaratan keamanan untuk suatu jenis produk. *File encryption* merupakan salah satu jenis produk yang merupakan hasil pengkajian dan pengembangan yang ada di BSSN dan dibutuhkan oleh para stakeholder. Pada makalah ini akan disusun *Protection Profile* untuk *File Encryption* berbasis *standalone* dimana dokumen ini dapat menjadi acuan bagi pengembang produk dalam memenuhi kebutuhan pengguna. Dokumen PP ini berisi sekumpulan rekomendasi persyaratan keamanan untuk *file encryption* yaitu *cryptographic key management, cryptographic operation*, *user identification before any action, user authentication before any action, audit data genenation, audit data review* dan *user initiated terminatioEvaluation Assurance Level (EAL)* yang dipilih yaitu EAL 2.

Kata Kunci: Protection Profile, File Encryption, SNI ISO/IEC 15408:2014, ISO/IEC TR 15446:2017, Keamanan, EAL2

1. PENDAHULUAN

Pelaksanaan pemantauan dan pengendalian produk keamanan siber dan sandi merupakan salah satu tugas pokok dan fungsi Deputi Bidang Pemantauan dan Pengendalian [1]. Pemantauan dan pengendalian ini diwujudkan dalam fasilitasi standardisasi dan sertifikasi modul sandi dan keamanan perangkat TI. Fasilitasi standardisasi keamanan perangkat TI diwujudkan dalam penyusunan *Protection Profile (PP)*. PP adalah dokumen standar keamanan suatu tipe *Target of Evaluation (TOE)* tertentu sesuai dengan tingkat jaminan keamanan yang ingin dicapai dalam sertifikasi TOE yang ditentukan [2]. TOE adalah produk teknologi informasi yang menjadi objek sertifikasi sesuai ISO/IEC 15408 dan ISO/IEC 18045 [2].

Produk TI adalah perangkat lunak dan/atau perangkat keras yang menyediakan fungsionalitas dan dirancang untuk digunakan atau diintegrasikan dalam sistem teknologi informasi [2]. *File encryption* adalah salah produk TI yang dikembangkan oleh Badan Siber dan Sandi Negara untuk memenuhi kebutuhan *stakeholder* dalam mengamankan *digital file* yang dipunyai *stakeholder.* Sebagai bentuk standardisasi terhadap persyaratan keamanan *file encryption* maka pada makalah ini akan dideskripsikan penyusunan dokumen PP untuk *file encryption* berdasarkan SNI ISO/IEC 15408:2014 [3] yang merupakan standar yang berisi persyaratan keamanan pada produk TI. Pada makalah ini yang menjadi TOE adalah aplikasi *File encryption* yang bersifat *stand alone.*

2. METODOLOGI PENELITIAN

2.1 Penyusupan Dokumen PP

Penyusunan dokumen PP mengikuti tahapan pada ISO/IEC TR 15446 – *Information technology – Security techniques – Guidance for the production protection profiles and security targets* **[4]**. Tahapan tersebut adalah:

a. Menentukan permasalahan keamanan.
b. Menentukan tujuan keamanan untuk mengatasi permasalahan keamanan.
c. Menentukan spesifikasi keamanan untuk memenuhi tujuan keamanan.
d. Menentukan fungsi keamanan untuk memenuhi persyaratan keamanan.
e. Menentukan *Evaluation Assurance Level (EAL)* dan *Security Assurance Requirements (SAR)*

Untuk menentukan EAL dan SAR, pada makalah ini digunakan *Matriks Degree of Robustness* **[5]**. Matriks ini mendefinisikan tingkat kekuatan dan penjaminan yang direkomendasikan untuk mekanisme keamanan. Penentuan EAL dan SAR didasarkan pada nilai informasi dan ancaman terhadap informasi yang dilingdungi oleh TOE. Terdapat lima kategori nilai informasi dan tujuh kategori ancaman, Setelah ditentukan posisi nilai informasi dan ancaman, selanjutnya dipilihlah EAL yang tepat sesuai dengan tabel berikut:

Tabel 1. Matriks *Degree of Robustness*

Nilai Informasi	Tingkat Ancaman						
	T1	T2	T3	T4	T5	T6	T7
V1	EAL1	EAL1	EAL1	EAL2	EAL2	EAL2	EAL2
V2	EAL1	EAL1	EAL1	EAL2	EAL2	EAL3	EAL3
V3	EAL1	EAL2	EAL2	EAL3	EAL3	EAL4	EAL4
V4	EAL1	EAL2	EAL3	EAL4	EAL5	EAL5	EAL6
V5	EAL2	EAL3	EAL4	EAL5	EAL6	EAL6	EAL7

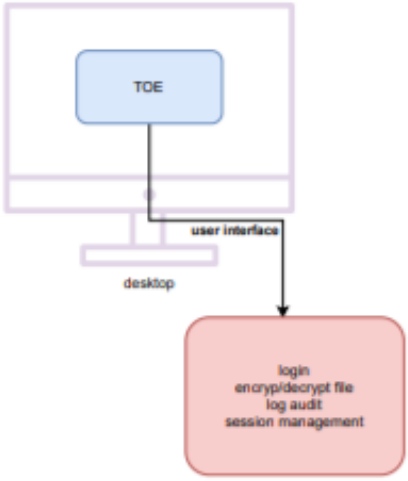
ISBN: 978-623-93614-6-4
Agustus 2021
Hal: 103 - 107

2.2 SNI ISO/IEC 15408:2014

Persyaratan fungsi keamanan atau *Security Functional Requirements (SFR)* merupakan fungsi keamanan yang diterapkan pada produk TI. SNI ISO/IEC 15408:2014 merupakan standar nasional untuk yang dapat menjadi acuan untuk penentuan fungsi keamanan tersebut [3]. Spesifikasi keamanan ini dapat berupa audit keamanan, dukungan kriptografi, identifikasi dan otentikasi, manajemen keamanan, akses terhadap prduk. dan lain sebagainya. Berikut adalah beberapa contoh fungsi keamanan sesuai standar tersebut.

3. HASIL DAN PEMBAHASAN

Sebelum melaksanakan langkah – langkah penyusunan PP, maka perlu didefinisikan TOE beserta ruang lingkupnya. TOE pada makalah ini adalah aplikasi *file encryption* yang bersifat *stand-alone* dan diinstall pada *desktop.* Sehingga seluruh persyaratan keamanan akan dilakukan pada TOE. Berikut adalah tampilan lingkup fisik dari TOE.
Gambar 1 dibawah ini memperlihatkan bahwa TOE akan diinstal pada *desktop* dan *user* dapat berinteraksi dengan TOE melalui *user interface*. *User* akan melakukan *login* sebelum dapat mengoperasikan TOE. Selanjutnya setelah berhasil login maka *user* dapat melakukan enkripsi dan dekripsi terhadap *digital file*. Selain itu *user* juga dapat melihat *log audit* yang berisi informasi mengenai siapa saja yang telah *login*, waktu dan status *login.* User dapat mengakhiri operasional TOE dengan menutup aplikasi



Gambar 1. Lingkup Fisik TOE

Setelah mendefinisikan ruang lingup TOE maka dimulailah penyusunan persyaratan keamanan berdasarkan tahapan pada ISO/IEC TR 15446 yaitu:

3.1 Menentukan Permasalahan Keamanan

Tahap ini bertujuan untuk menentukan ruang lingkup permasalahan keamanan yang ditangani oleh produk TI yang selanjutnya pada makalah ini disebut *Target of Evaluation* (TOE). Permasalahan keaanan ini terdiri dari asumsi, ancaman dan kebijakan organisasi.

3.1.1 Asumsi

Asumsi yang ditentukan terkait dengan lingkungan dimana TOE dioperasionalkan. Tabel 2 menunjukkan asumsi tersebut.

Tabel 2. Asumsi

Asumsi	Penjelasan
A.LINGK	Asumsi ini terkait dengan lingkungan operasional TOE harus aman dan dikelola dengan baik.
A.USER	Asumsi ini terkait dengan pengguna TOE telah mendapatkan pelatihan terkait penggunaan TOE dan informasi relevan lainnya.
A.SOP	Asumsi ini terkait dengan keberadaan SOP yang mendukung operasional TOE telah disusun dan disahkan.
A.KONEK	Asumsi ini terkait dengan konektivitas PC/desktop dimana TOE diinstalasi merupakan jaringan yang aman dan tepercaya..
A.SATU	Asumsi ini terkait dengan desktop dimana TOE diinstalasi hanya pada satu perangkat tersebut dan milik pengguna yang berwenang.
A.TMSTAMP	Asumsi ini terkait dengan tersedianya timestamp yang valid oleh *platform* dimana TOE diinstalasi.

3.1.2 Ancaman

Aset pada TOE adalah *password* dan *digital file*. Berbagai ancaman akan membahayakan asset. Namun demikian fungsi keamanan pada TOE harus melindungi asset tersebut. Tabel 3 menunjukkan ancaman yang dimaksud.

ISBN: 978-623-93614-6-4
Agustus 2021
Hal: 103 - 107

Tabel 3. Ancaman

Ancaman	Penjelasan
T. UNGKAP	Bertujuan untuk mendapatkan *ciphertext* dan mencoba untuk melakukan kriptanalisis padahal penyerang tidak mempunyai akses terhadap kunci.
T. TBKPSWDUSER	Bertujuan untuk menebak *password* untuk dapat mengakses TOE.
T. CREDENSIAL	Bertujuan untuk mendapatkan *credential data* berupa nilai *hashing* dari *password*
T. LOG	Bertujuan menghapus atau memodifikasi data audit.

3.1.3 Kebijakan Keamanan Organisasi

Tabel 4 yang menyatakan kebijakan keamanan organisasi yang harus mendukung operasional TOE.

Tabel 4. Kebijakan Organisasi

Kebijakan	Penjelasan
P. AKS	Mengatur TOE hanya diakses oleh pengguna yang terotorisasi
P. GNTPSWD	Mengatur pengguna agar mengganti *password* secara berkala
P. ATRPSWD	Mengatur pengguna untuk menggunakan *password* yang kuat

3.2 Menentukan Tujuan Keamanan

Tujuan keamanan TOE untuk mengatasi permasalahan keamanan yang telah ditentukan pada tahap sebelumnya. Tujuan kemanan ditentukan untuk TOE dan lingkungan operasionalnya.

3.2.1 Tujuan Keamanan untuk Lingkungan Operasional Non-IT dan IT

Berikut adalah tujuan kemanan untuk lingkungan operasional non-IT dan IT.

Tabel 5. Tujuan Keamanan untuk Lingkungan Operasional Non-IT dan IT.

Tujuan Keamanan yang Berhubungan dengan Lingkungan Operasional	Penjelasan
OE. USER	Pengguna TOE telah diberikan pelatihan terkait operasional TOE.
OE.SOP	Prosedur operasional TOE telah disusun dan disahkan oleh pihak yang berwenang.
OE. LING	TOE dioperasionalkan pada lingkungan yang aman dengan pengelolaan yang baik.
OE.KONEK	PC/desktop dimana TOE diinstalasi terkoneksi pada jaringan yang aman dari serangan.
OE.SATU	TOE hanya diinstalasi pada satu *desktop* yang dimiliki oleh *user* yang berwenang.
OE.TMSTAMP	*Platform* dimana TOE beroperasi menyediakan *timestamp* yang valid.

3.2.2 Tujuan Keamanan untuk TOE

Tabel 6 mendeskripsikan tujuan keamanan dari TOE.

Tabel 6. Tujuan Keamanan untuk TOE

Tujuan Keamanan untuk TOE	Penjelasan
O. RHS	TOE mengimplementasikan mekanisme untuk menjamin kerahasiaan *file digital.*
O. USERASLI	TOE mengimplementasikan mekanisme bahwa pengguna otentik yang mampu mengakses layanan TOE.
O. AUDIT	TOE membangkitkan log pada proses login
O. SESSION	TOE harus menyediakan session dan penutupan aplikasi dari *user*.
O.JAGACREDENSIAL	TOE harus mengimplementasikan mekanisme untuk menjaga *data credential* dari pihak yang tidak berwenang.

3.2.3 Menyusun Matriks Rasional Permasalahan Keamanan dan Tujuan Keamanan

Matriks rasional menunjukkan tujuan keamanan dari TOE berkorespondensi (ditunjukkan dengan tanda *check* (√)) untuk menanggulangi permasalahan keamanan. Berikut adalah Tabel 7 yang menunjukkan korespondensi tersebut.

Tabel 7. Matriks Rasional Permasalahan Keamanan dan Tujuan Keamanan

	T.UNGKAP	T.TBKPSWDUSER	T.CREDENSIAL	T.LOG	A.LINGK	A.USER	A.SOP	A.KONEK	A.SATU	A.TMSTAMP	P.AKS	P.GNTPSWD	P.ATRPSWD
O. RHS	√												
O. USERASLI		√									√	√	√
O. AUDIT				√									

ISBN: 978-623-93614-6-4
Agustus 2021
Hal: 103 - 107

	T.UNGKAP	T.TBKPSWDUSER	T.CREDENSIAL	T.LOG	A.LINGK	A.USER	A.SOP	A.KONEK	A.SATU	A.TMSTAMP	P.AKS	P.GNTPSWD	P.ATRPSWD
O. SESSION		√											
O.JAGACREDENSIAL			√										
OE. LINGK					√								
OE. USER		√	√	√		√							
OE.SOP							√						
OE.KONEK								√					
OE.SATU									√				
OE.TMSTAMP										√			

Setiap korespondensi kemudian dijelaskan dalam bentuk narasi agar didapatkan alasan yang kuat mengapa tujuan keamanan telah menjawab permasalahan keamanan. Berikut adalah tabel yang menunjukkan penjelasan tersebut:

Tabel 8 Deskripsi Justifikasi Permasalahan Keamanan dan Tujuan Keamanan

Permasalahan Keamanan	**Penjelasan**
T.UNGKAP	O.RHS mengharuskan TOE mengimplementasikan mekanisme untuk menjamin kerahasiaan *file digital*. T.UNGKAP diminimalisir dengan cara menjaga kerahasiaan *file* dengan melakukan enkripsi terhadap *file* tersebut. Seseorang yang tidak berwenang seharusnya tidak mendapatkan *file* aslinya Dengan demikian T.UNGKAP dapat diminimalisir dengan O.RAHASIA.
T.TBKPSWDUSER	O.USERASLI mengharuskan TOE mengimplementaiskan mekanisme bahwa pengguna otentik yang mampu mengakses layanan TOE. T.TBKPSWDUSER diminimalisir dengan cara *user* otentik dibuktikan dengan kepemilikan *username* dan *password* yang sah agar berhasil login pada TOE. O.SESSION mensyaratkan TOE harus menyediakan session dan penutupan aplikasi dari *user* sehingga *user* yang berwenang saja yang dapat masuk dan mengoperasikan TOE P.AKSES merupakan kebijakan yang mengatur TOE hanya diakses oleh pengguna yang terotorisasi. P.GNTPSWD merupakan kebijakan yang mengatur pengguna agar mengganti password secara berkala. P.ATRPSWD merupakan kebijakan yang mengatur pengguna untuk menggunakan password yang kuat. OE.USER mensyaratkan bahwa pengguna TOE telah diberikan pelatihan terkait operasional TOE. Dengan demikian T.TBKPSWDUSER diminimalisir oleh O.USERASLI ,P.AKSES, P.GNTPSWD, P.ATRPSWD, dan OE.USER.
T.CREDENSIAL	O.JAGACREDENTSAL mengharuskan TOE harus mengimplementasikan mekanisme untuk menjaga *data credential* dari pihak yang tidak berwenang. T.CREDENSIAL diminimalisir dengan mekanisme pengamanan berupa enkripsi pada *data credential*. OE.USER mensyaratkan bahwa pengguna TOE pelatihan terkait operasional TOE termasuk bagaimana cara menjaga *data credential*. Dengan demikian T.CREDENSIAL diminimalisir oleh O.JAGACREDENSIAL dan OE.USER.
T.LOG	O.AUDIT mengharuskan TOE membangkitkan log pada proses login. T.LOG diminimalisir dengan mekanisme pengamanan yaitu enkripsi pada *log audit*. OE.USER mensyaratkan bahwa pengguna TOE telah mendapatkan pelatihan terkait operasional TOE. Dengan demikian T.AUDITLOG diminimalisir oleh O.AUDIT dan OE.USER.
A.LINGK	OE.LINGK mengharuskan lingkungan operasional TOE aman dan dikelola dengan baik. Sehingga OE.LINK memenuhi asumsi A.LINK.
A.USER	OE.USER mengharuskan bahwa pengguna telah diberikan pelatihan terkait operasional TOE. Sehingga OE.USER memenuhi asumsi A.USER.
A.SOP	OE.SOP mengharuskan prosedur operasional TOE telah disusun dan disahkan oleh pihak yang berwenang. Sehingga OE. SOP memenuhi asumsi A. SOP.
A.KONEK	OE.KONEK mengharuskan PC/desktop dimana TOE diinstalasi terkoneksi pada jaringan yang aman dari serangan. Sehingga OE.KONEK memenuhi asumsi A. KONEK.
A.SATU	OE.SATU mengharuskan TOE hanya diinstalasi pada satu desktop yang dimiliki oleh user yang berwenang. Sehingga OE.SATU memenuhi asumsi A. SATU.
A.TMTAMP	OE.TMSTAMP mensyaratkan Platform dimana TOE beroperasi menyediakan *timestamp* yang valid. Sehingga OE.TMSTAMP memenuhi asumsi A. TMSTAMP.
P.AKS	O.USERASLI mengharuskan TOE mengimplementasikan mekanisme bahwa pengguna otentik yang mampu mengakses layanan TOE. Pengguna harus mempunyai *username* dan *password* yang sah untuk melakukan *login* dengan sukses

ISBN: 978-623-93614-6-4
Agustus 2021
Hal: 103 - 107

Permasalahan Keamanan	Penjelasan
P.GNTPSWD	Sehingga O.USERASLI menjalankan kebijakan P.AKSES bahwa TOE hanya diakses oleh pengguna yang berhak. O.USERASLI mengharuskan TOE mengimplementasikan mekanisme bahwa pengguna otentik yang mampu mengakses layanan TOE. Pengguna harus mempunyai *username* dan *password* yang sah untuk dapat *login*. Pengguna akan melakukan penggantian *password* secara berkala. O.USERASLI menjalankan kebijakan P.GNTPSWD bahwa pengguna harus melakukan penggantian *password* secara teratur.
P.ATRPASWD	O.USERASLI mengharuskan TOE mengimplementasikan mekanisme bahwa pengguna otentik yang mampu mengakses layanan TOE. Pengguna harus mempunyai *username* dan *password* yang berkesesuaian untuk dapat *login*. Pengguna akan melakukan pengaturan *password* yang kuat. O.USERASLI menjalankan kebijakan P.ATRPSWD bahwa pengguna otentik harus menggunakan *password* yang kuat.

3.3 Menentukan SFR yang Sesuai Berdasarkan Tujuan Keamanan

Setelah dilakukan penelusuran seluruh permasalahan keamanan telah ditangani oleh setidaknya satu tujuan keamanan, maka dilakukanlah pemilihan SFR sesuai dengan tujuan keamanan tersebut. *Cryptographic key management* dan *cryptographic operation* merupakan SFR yang sesuai untuk O.RAHASIA dan O.JAGACREDENSIAL. *User identification and user authentication before any action* merupakan SFR yang sesuai untuk O.USERASLI. *Audit data genenation* dan *audit data review* merupakan SFR yang sesuai untuk O.AUDIT. *User initiated termination* merupakan SFR yang sesuai untuk O.SESSION.

3.4 Penentuan *Evaluation Assurance Level (EAL) dan Security Assurance Requirements (SAR)*

Berdasarkan Matriks *Degree of Robustness* maka nilai informasi yang dilindungi TOE berada pada nilai V3 yaitu jika informasi yang dilindungi bocor maka akan menyebabkan beberapa kerusakan terhadap keamanan, keselamatan, postur finansial atau infrastruktur organisasi. Sedangan tingkat ancaman berada pada T3 yaitu oenyerang dengan sumber daya minimal yang bersedia mengambil risiko signifikan. Sehingga EAL yang dipilih adalah EAL 2. *Package* EAL 2 berdasarkan SNI ISO/IEC 15408:2014 Bagian 3[4].

4. KESIMPULAN

Telah dilakukan perancangan *Protection Profile File Encryption* berdasarkan SNI ISO/IEC 15408:2014. Spesifikasi keamanan yang telah dirancang adalah *cryptographic key management, cryptographic operation, user identification before any action, user authentication before any action, audit data genenation, audit data review* dan *user initiated termination*. EAL yang dipilih adalah EAL 2.

REFERENCES

[1] B. S. d. S. Negara, "Jaringan Dokumentasi dan Informasi Hukum BSSN," 2020. [Online]. Available: https://jdih.bssn.go.id/arsip-hukum/peraturan-badan-siber-dan-sandi-negara-nomor-9-tahun-2020-tentang-organisasi-dan-tata-kerja-badan-siber-dan-sandi-negara.
[2] B. S. d. S. Negara, "Jaringan Dokumentasi dan Informasi Hukum BSSN," 2019. [Online]. Available: https://jdih.bssn.go.id/arsip-hukum/peraturan-badan-siber-dan-sandi-negara-nomor-15-tahun-2019-tentang-penyelenggaraan-skema-common-criteria-indonesia.
[3] B. S. Nasional, "SNI ISO/IEC 15408:2014," Badan Standardisasi Nasional, Jakarta, 2014.
[4] B. S. Nasional, "ISO/IEC TR 15446:2017," ISO Central Secretariat, Jakarta, 2017.
[5] B. Prayitno, "Pengembangan Protection Profile dan Security Target untuk Module Operation of Security Component (MOSC) Meter Listrik Prabayar Komunikasi Dua Arah (MLPKDA) Berdasarkan Common Criteria Versi 3.1 Revisi 4," Institut Teknologi Bandung, Bandung, 2017.